SLAUGHTER AND MAY/

February 2024

CHANGE IS AFOOT FOR CYBER GOVERNANCE

For some time we have been saying that cyber risk, like all business risks, is ultimately a corporate governance issue. Whilst the CISO / IT team have responsibility in the risk register, it is the board who has responsibility for setting risk appetite and for the ultimate oversight of the management of this risk. This is not universally reflected in the business world however, as shown in a Marsh global survey in which 70% of respondents named IT as the primary owner and decision-maker for cyber risk management, compared to 37% who cited the C-suite. That said, this view needs to change given recent developments.

UK Corporate Governance Code

The updated UK Corporate Governance Code published on 22 January 2024 introduces a new concept that boards should establish and maintain an effective risk management and internal control framework. Given that cyber security is either a principal risk, or is relevant to an organisation's management of principal risks, for most organisations, the changes to the Corporate Governance Code squarely puts responsibility for cyber risk in the board's court.

Guidance on the UK Corporate Governance Code was subsequently published by the Financial Reporting Council on 29 January 2024. This guidance explains, for instance, that the board should:

- determine the nature and extent of the principal risks and its risk appetite;
- agree how the principal risks should be managed or mitigated to reduce the likelihood of their incidence or their impact;
- monitor and review the risk management and internal control systems, and the management's process for this, and satisfy itself that they are functioning effectively, and that corrective action is being taken where necessary; and
- ensure effective external communication on risk management and internal control.

Draft Cyber Governance Code of Practice

However, it is not clear that all boards currently know what good cyber governance looks like in practice, with the UK Government's 2023 Cyber Breaches Survey noting that "there is a lack of understanding of what constitutes effective cyber risk management".

It is therefore helpful that the Government also published a draft Cyber Governance Code of Practice (23 January 2024) on which it is seeking views. This aims to support directors to drive greater cyber resilience.

The Code consists of five overarching principles, with each having relevant actions attributed to it. By necessity these are not unduly prescriptive to ensure that they have broad applicability and so there is still much scope for variation in their application.

These principles and actions are summarised below:

1. Risk management

Actions include ensuring that cyber risks should be addressed as part of the organisation's broader enterprise risk management and internal control activities, and establishing ownership of risks with relevant senior managers beyond the CISO.

2. Cyber strategy

This covers monitoring the cyber resilience strategy and its delivery, and ensuring the allocation of appropriate resources.

3. People

This principle focusses on communications and training. It includes ensuring that there are effective and measurable cyber security training and awareness programmes in place, and sponsoring communications on the importance of cyber resilience.

4. Incident planning and response

The associated actions include that the board should ensure that the organisation has a cyber incident plan and that there is at least annual testing of it. Additionally, in the event of an incident, the board should support executives in critical decision making and external communications.

5. *Assurance and oversight*

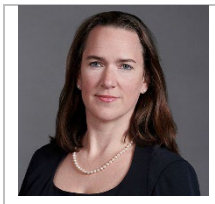
This principle requires the board to establish a governance structure with clear roles and responsibilities and ownership of cyber at director level. It specifies that there should be formal reporting at least quarterly, with regular dialogue with the CISO and other relevant executives.

The Code is intended to reflect existing best practice and to complement existing industry and government resources, both in the UK and internationally. Many directors will already be familiar with the Cyber Security Toolkit for Boards published by the National Cyber Security Centre (see our blog), and the intention is that the Code and the Toolkit will work together to form a coherent set of guidance for boards.

Once in final form, the Government's current intention is that the Code be launched as a voluntary tool, without its own statutory footing. However, investors are increasingly focussed on governance of cyber, with Glass Lewis (an influential proxy voting firm) having last year added a new section to its proxy voting guidelines stating that "a company's stakeholders would benefit from clear disclosure regarding the role of the board in overseeing issues related to cybersecurity".

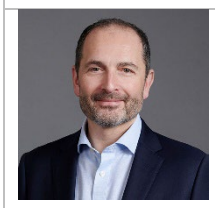
It can therefore be expected that, even if the Code is voluntary, investor expectations (and concerns over individual director liability) will drive boards to follow it regardless of its voluntary nature.

Slaughter and May's cyber hub supports clients on both cyber preparedness and incident response. We have advised on some of the highest profile cyber attacks in the UK and internationally. If you have any cyber related questions, please contact one of our team below or your usual Slaughter and May contact.



REBECCA COUSIN
PARTNER
T: 020 7090 3049
E: Rebecca.Cousin@slaughterandmay.com

NATALIE DONOVAN
COUNSEL PSL, HEAD OF KNOWLEDGE TECH AND DIGITAL
T: 020 7090 4058
E: Natalie.Donovan@slaughterandmay.com



ROB SUMROY
PARTNER
T: +44 (0)20 7090 4032
E: Rob.Sumroy@slaughterandmay.com

JONATHAN COTTON
PARTNER
T: 020 7090 4090
E: Jonathan.Cotton@slaughterandmay.com